AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY
1 Martin Place (Level 12), Sydney, NSW 2000
GPO Box 9836, Sydney, NSW 2001

T 02 9210 3000 | W www.apra.gov.au

Additional support information for submitting applications to register accountable persons

- D2A Guide for Submitting ARF 550.0 is provided in Appendix 1.

- Common BEAR submission errors to avoid are listed in Appendix 2.

- Naming conventions to be used for BEAR documents are available in Appendix 3.

- A guide to using SecureDoc and SecureDoc Technical FAQs is provided in Appendix 4.

- Entities requiring further guidance regarding the BEAR registration processes can contact APRA by email at DataAnalytics@apra.gov.au.

- Entities requiring technical support for SecureDoc, including adding or removing individuals' access to the BEAR folder in SecureDoc are to contact APRA by email at DataAnalytics@apra.gov.au.

- Entities requiring further assistance with these BEAR guidelines or in response to requests for additional information should contact the responsible supervisor.

Appendix 1 D2A Guide for Submitting ARF 550.0

Initial Submission (BEAR Baseline Return)

Entities must submit the BEAR Baseline return via D2A by 14 June 2019. The BEAR Baseline return will be available to submit from 20 May 2019 and we encourage ADIs to submit as soon as you have received draft feedback from your supervisor and are ready to submit.

These following instructions are for the initial ARF 550.0 submission:

1. Open D2A.
2. Enter your security details (AUSkey details).
3. Open the ARF550.0 form, complete, and validate the return.
4. If any errors are detected, a pop-up box with the error details will be displayed. Correct all errors displayed.
5. From the file menu select ‘submit’, or click the ‘submit’ icon in the toolbar.
6. Enter your security details (AUSkey details) and click ‘OK’.
7. If no errors are detected during the submission you will receive a reference number. Please keep a note of this reference number.
8. Click close.

When the data has been received by APRA, a confirmation email is sent to the e-mail address registered to your D2A installation. You can check the registered email address in D2A by opening the about window in the help menu. D2A needs to be re-installed to change this email address.

Resubmissions made until 14 June 2019 (BEAR Baseline Return modifications)

After the initial submission, if amendments need to be made to the information provided, the Baseline Return can be resubmitted up until 14 June 2019. The ability to amend a prior resubmission will cease from Monday 17 June.*

The following instructions are for resubmitting the initial ARF 550.0 form provided under the BEAR Baseline Return:

1. Open D2A.
2. Enter your security details (AUSkey details).
3. From the tools menu select ‘get data’, or click the ‘get data’ icon in the toolbar.
4. Enter your security details (AUSkey details) and click ok.
5. In the return chooser, select the ‘BEAR Baseline Return’, select the last submitted ARF 550.0 form, then click ‘download’
6. When the download is complete, you should see all the information submitted so far. click ok
7. Make the amendments as required and validate the return. If any errors are detected, a pop-up box with the error details will be displayed. Correct all errors displayed.
8. From the file menu select ‘submit’, or click the ‘submit’ icon in the toolbar.
9. Enter your security details (AUSkey details) and click ‘ok’.
10. If no errors are detected during the submission you will receive a reference number. Keep a note of this reference number.
11. Click Close.

Subsequent submissions made post 14 June 2019

To register additional persons or make changes to previous registrations after 14 June 2019, an ad-hoc BEAR Return will need to be submitted.*

To obtain an ad-hoc BEAR return, send a request to APRA via email (DataAnalytics@apra.gov.au) to allocate an ad-hoc BEAR Return.

These are the instructions to submit an ad-hoc ARF 550.0 pre-populated form:

1. Open D2A.
2. Enter your security details (AUSkey details).
3. From the Tools menu select 'return all blank forms'. A pop-up box appears showing the progress. Once the refresh is completed, click 'ok'.
4. From the file menu, select 'new'.
5. Open the ARF 550.0 form. The form will open with all the information that you have previously submitted to APRA.
6. Update the form as required and validate the return.
7. If any errors are detected, a pop-up box with the error details will be displayed. Correct all errors displayed.
8. From the File menu select 'submit', or click the 'submit' icon in the toolbar.
9. Enter your security details (AUSkey details) and click ok.
10. If no errors are detected during the submission you will receive a reference number. Please keep a note of this reference number.
11. Click Close.

When the data has been received by APRA, a confirmation email is sent to the email address registered to your D2A installation. You can check the registered email address in D2A by opening the about window in the help menu. D2A needs to be re-installed to change this email address.

*** Note**: As the last day to modify ARF 550.0 submissions is a Friday (14 June) and the ad-hoc BEAR return will not be available until the following Monday (17 June), APRA will accept Baseline returns submitted or resubmitted on the weekend of 15 and 16 June 2019.

Appendix 2 Common BEAR Submission Errors

Error	Solution
BEAR documents emailed to the responsible supervision team or the Accountability Regime email address.	All BEAR documents to be submitted via SecureDoc. A dedicated team processes submissions received via SecureDoc. General correspondence such as questions should be emailed to your responsible supervisor.
Documents uploaded to the incorrect SecureDoc folder.	Some ADIs use SecureDoc for other purposes, including for sending some information to their responsible supervisor. Please use only the BEAR folder for BEAR submissions.
Document file names not adhering to the naming conventions provided.	Using the naming conventions in Appendix 3 ensures ADIs and APRA can identify relevant documents in the future when required.
Invalid characters contained in file names such as /, * # & … etc.	Follow the naming convention outlined in Appendix 3.
Supporting documents (accountability statements, accountability maps, etc.) submitted as one single document.	Each document needs to be submitted as a separate file adhering to the naming convention outlined in Appendix 3.

Appendix 3

BEAR Document Naming Conventions Guide

Document Type	Naming convention	Example Document Name
Accountability statement	<Document type> <name of entity> <name of individual> <effective date>	Accountability Statement ABC Bank Ann Blog 18012019
Accountability Map	<Document type> <name of entity> <effective date>	Accountability Map ABC Bank 18012019
Documents supporting Accountable Person Registration (if needed)	<Document Type> <name of entity> <name of individual> <effective date>	Supporting Document Accountability Statement ABC Bank Ann Blog 18012019
Documents supporting Accountability maps (if needed)	<Document Type> <name of entity> <effective date>	Supporting Document Accountability Map ABC Bank 18012019
Documents supporting Breach Notification (if needed)	<Document Type> <name of entity> <name of individual> <date of notification>	Supporting Document Breach Notification ABC Bank Jill Blog 20032019

Appendix 4

Guide to using SecureDoc and SecureDoc Technical FAQs

Adding and removing staff access to your Entity SecureDoc folder

Access to view and upload documents in your entities SecureDoc folder is managed by APRA.

To grant access to a staff member, please email the staff members' full name, role title, and their entity email address to DataAnalytics@apra.gov.au, requesting they be granted access to your entities folder. Once APRA adds their address to the entity folder, they will be notified by an email.

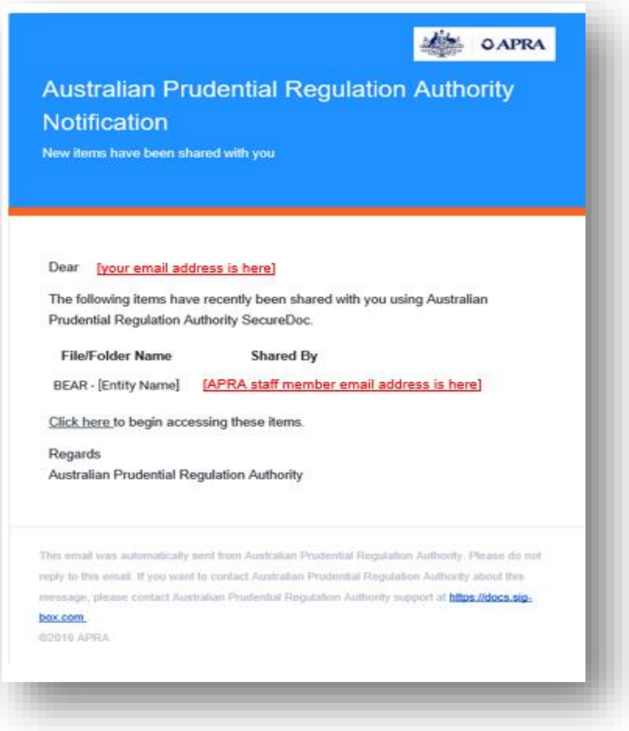
To remove access from a staff member, please advise the staff member's full name and entity email address to DataAnalytics@apra.gov.au, and request that they be removed from the list of staff with access permission.

Accessing SecureDoc

Step 1 First time User (existing users go to step 2 over the page)

Once an email address has been granted permission to access the entity folder in SecureDoc, the staff member will receive two emails. Only action Email 2:

Email 1:



Australian Prudential Regulation Authority Notification

New items have been shared with you

Dear [your email address is here]

The following items have recently been shared with you using Australian Prudential Regulation Authority SecureDoc.

File/Folder Name	Shared By
BEAR - [Entity Name]	[APRA staff member email address is here]

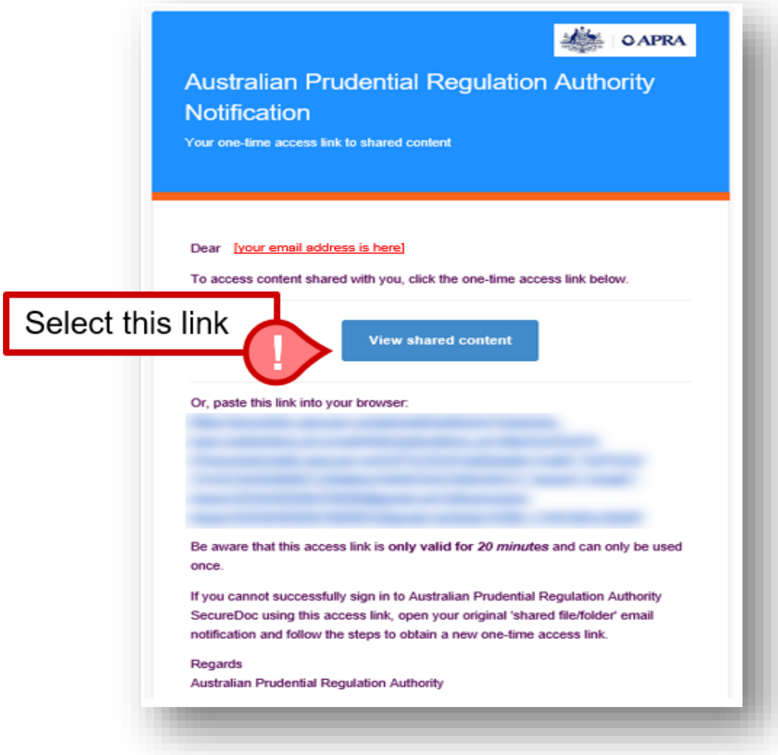
Click here to begin accessing these items.

Regards
Australian Prudential Regulation Authority

This email was automatically sent from Australian Prudential Regulation Authority. Please do not reply to this email. If you want to contact Australian Prudential Regulation Authority about this message, please contact Australian Prudential Regulation Authority support at https://docs.sig-box.com

©2016 APRA

Email 2: (action this email if you are a first time user)



Australian Prudential Regulation Authority Notification

Your one-time access link to shared content

Dear [your email address is here]

To access content shared with you, click the one-time access link below.

Select this link

Or, paste this link into your browser:

[redacted]

Be aware that this access link is only valid for *20 minutes* and can only be used once.

If you cannot successfully sign in to Australian Prudential Regulation Authority SecureDoc using this access link, open your original 'shared file/folder' email notification and follow the steps to obtain a new one-time access link.

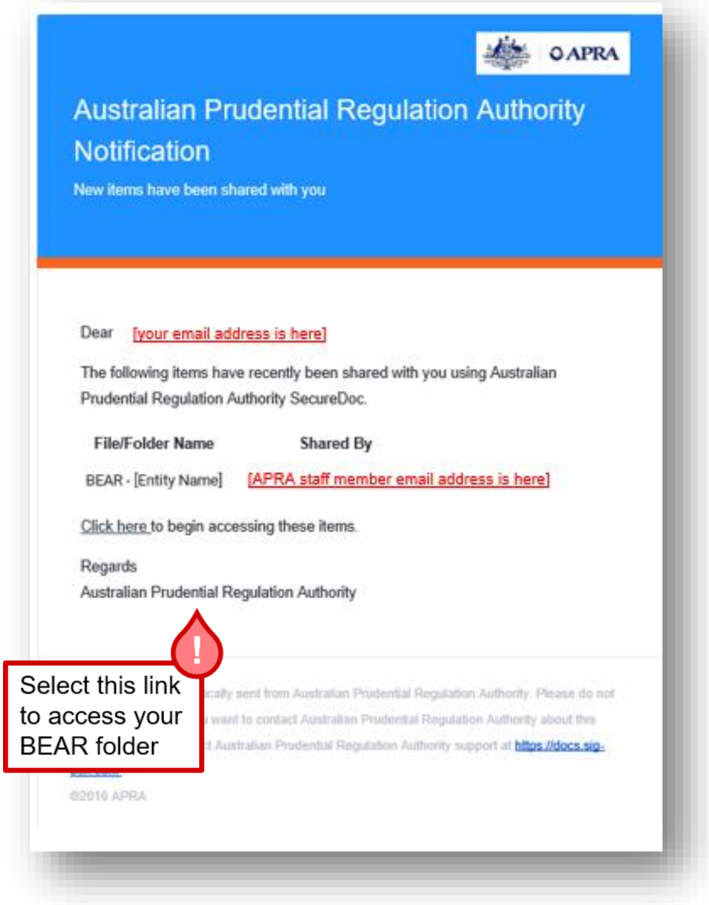
Regards
Australian Prudential Regulation Authority

1. After selecting the link pictured, you will be prompted to create a password (passwords must be a minimum of 12 characters and contain characters from at least 2 of the following character sets: lowercase letters, uppercase letters, numbers, symbols).

2. Once your password has been set, SecureDoc can be accessed via https://securedocstatic.apra.gov.au. It is recommended regular users save this link.

Step 2 Existing Users

1. An APRA staff member will grant you with access to a folder within SecureDoc which has been specifically created for your entities BEAR documentation. When this occurs you will receive the email below. Click on the ‘click here’ link to begin accessing the folder.



APRA

Australian Prudential Regulation Authority Notification

New items have been shared with you

Dear [your email address is here]

The following items have recently been shared with you using Australian Prudential Regulation Authority SecureDoc.

File/Folder Name	Shared By
BEAR - [Entity Name]	[APRA staff member email address is here]

Click here to begin accessing these items.

Regards
Australian Prudential Regulation Authority

...cally sent from Australian Prudential Regulation Authority. Please do not ...u want to contact Australian Prudential Regulation Authority about this ...d Australian Prudential Regulation Authority support at https://docs.sig-

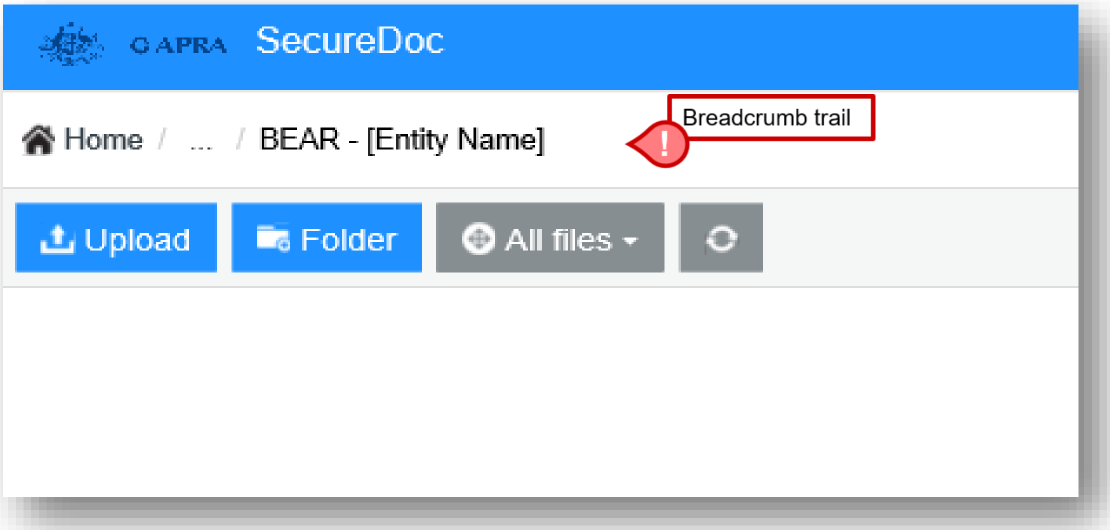
©2016 APRA

Select this link to access your BEAR folder

2. Alternatively, once you receive the email above you can access your BEAR folder by logging into SecureDoc via https://securedocstatic.apra.gov.au using your existing account log in details.

Uploading BEAR documents to APRA via SecureDoc.

1. Log in to your SecureDoc account and navigate to the BEAR folder for your entity. Your location in SecureDoc can be identified from the breadcrumb trail.



2. Documents can be uploaded via the **Upload** button in the SecureDoc toolbar or via drag-and-drop. **Please ensure documents are named according to the advised naming conventions.** A copy of the naming conventions is available at the end of this document.

3. Multiple documents can be uploaded simultaneously.

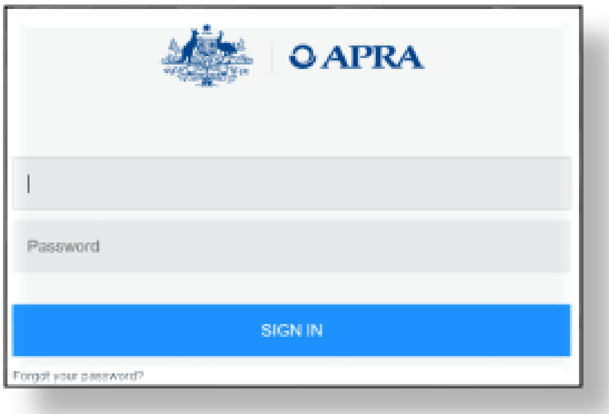
4. APRA will be notified once these documents have been uploaded. They will be removed from SecureDoc once actioned. SecureDoc is not to be used as a data storage facility.

SecureDoc FAQ (Technical)

What is SecureDoc?

APRA SecureDoc is a web based file sharing solution. It is a dedicated instance of ‘Covata Safe Share’ and hosted by Macquarie Government’s PROTECTED government cloud enclave. Macquarie call the product ‘SigBox’.

When an authorised user uploads data using their browser it is transparently encrypted using unique cryptographic keys for each file. Files are encrypted within the application and when synchronized to an end-user device. Data is not decrypted until the authorised users view it on their devices. Access controls can determine which users can view, download, and edit sensitive information.



Does the Web server, application server and database all reside on the same hardware infrastructure or is it a 3-tier system?

Yes it does. See the overview diagram below.

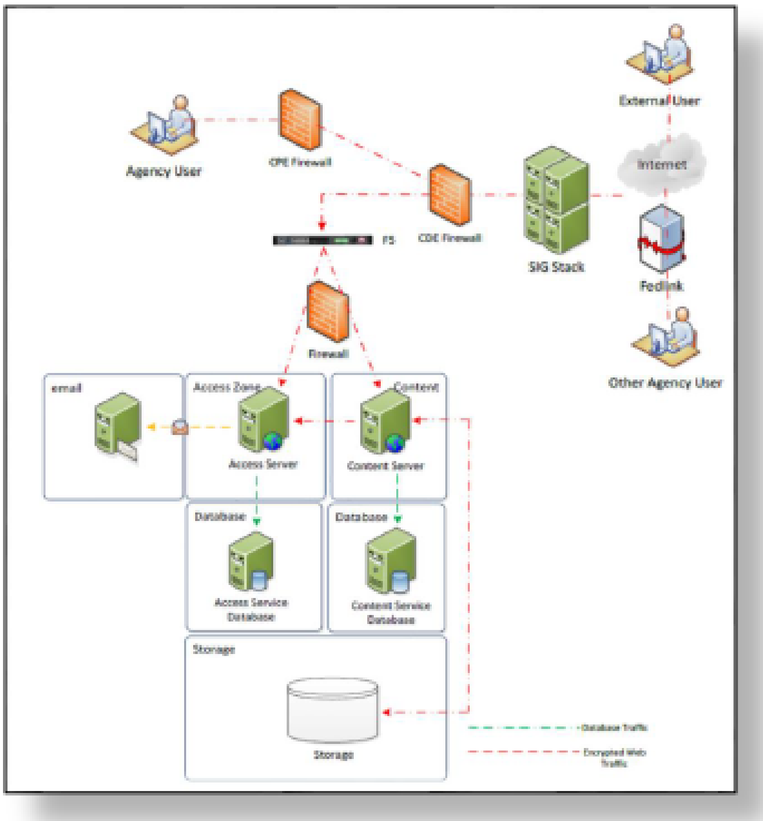
If all components are on the same hardware, how are they secured?

SecureDoc separates access and content services. Data is stored separately from the web application and is decrypted in the browser after TLS transmission.

Below is more information on the two services used by the Covata Platform.

1. The Access Service manages authentication, authorization, keys, access controls, auditing and the Meta data. This component handles all aspects of managing and controlling the encrypted data, it does not have any direct access to either the unencrypted or encrypted data itself.

2. The Content Service is responsible for the management of user’s data. This component passes files between the cloud store and user. It also generates difficult to copy rendered views of the data content for ‘view only’ file distribution.



Are uploaded documents scanned for malware?

No. SecureDoc doesn't scan for malware.

How are user accounts managed?

APRA's security team reviews 'originator' user accounts on a regular basis.

Accounts created by APRA users for other contributors, such as entity contacts and third parties, cannot create or connect to folders that have not been shared with them.

No automated account management occurs.

The recommended practice is for 'originators' to create a folder per review / consultation. Once the review is complete, the shared folder should be deleted. This practice ensures that SecureDoc is not used as a document repository and user access is removed in a timely fashion.

How do I know what users are doing?

User activity monitoring is accessible by the owners of the folder/file via the history tab. APRA Administrators can see the logged activity on a folder or file but they cannot see the content of the file/folder.

Do you have periodic Vulnerability scans and penetration testing done? And is the penetration testing done by an independent third party?

APRA conducts regular vulnerability scans of our internal/external networks.

We have regular external pen tests conducted on our outward facing websites. In addition, Covata conduct an annual pen test on their application and notify customers about updates, patches or changes.

I have more technical / security questions, who should I ask?

Please contact secure@apra.gov.au

AES256 is used for end-to-end encryption for files stored at rest.

What security measures have been implemented to protect the Database from unauthorised access?

An "iRAP" assessment has been completed, which assures that the system and supporting processes comply with the Australian Government Information Security Manual (ISM) to a PROTECTED level. Storage is isolated in a PROTECTED cloud enclave. Please see the ASD website for more information about IRAP. https://asd.gov.au/infosec/irap.htm

Each folder is encrypted with an individual key associated with the folder owner. Only the owner of the folder (and the persons they share the folder with) can view the contents. Each file is individually encrypted.

How are user credentials protected?

Credentials are stored in the access service database. Limited Administrators have access to the user names, which are email addresses and contact details but not the encrypted passwords. Actions against accounts are logged.

How are users authenticated to upload documents?

Users need to login in order to upload documents.